IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Scott C. Harris	Group Art Unit 3662
Appl. No.	:	10/065,120	
Filed	:	September 18, 2002	
For	:	POSITION PRIVACY IN AN ELECTRONIC DEVICE	
Examiner	:	G. Issing	

Mail Stop AF
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

APPLICANTS BRIEF ON APPEAL

Sir:

Applicant herewith files this Appeal Brief under 37 C.F.R. 41.37 complying with the notice of to perfect the notice of appeal filed June 19, 2008. The sections required by the rules follow. No fee should be necessary since the fee was paid with the appeal brief filed August 8, 2005, in which no decision on the merits was issued.

This appeal brief was originally filed on August 19, 2008, and is resubmitted per the notification of non-compliant brief mailed August 28, 2008.

Real Party In Interest

Scott C. Harris, the inventor, is the real party in interest

Related Appeals and/or Interferences

There are no known related appeals and/or interferences

Status of Claims

Claims 1-2, 4-7, 9-13, 15-20, 23-27 and 51 and 52 are pending.

Each of these claims1-2, 4-7, 9-13, 15-20, 23-27 and 51 and 52 are rejected. Each of these claims are being appealed.

The claims 3,8,14,16,21,22,28,35-50 have been cancelled and are not being appealed.

Status of Amendments

No amendment was filed subsequent to the March 20, 2008 final rejection.

Summary of Claimed Subject Matter

Claim 1 requires a cellular phone that has a position detection module which determines the position of the cellular phone and reports information indicative of the position. The positioning device 210 is described on page 2 of the specification, seventh line from the bottom. The position detector is described as being able "to determine its position and report that position to a remote source..." page 2, last two lines.

Claim 1 also defines a security part that is actuated to enhance privacy, and which produces a signal state that prevents the position detection module from determining its position for one embodiment, this can read on a number of embodiments, including the condition block control 220 which can "deactivate the function of the positioning device 210". See page 2 fourth line from the bottom. Other embodiments may include the cover 350 described page 4 beginning at line 10 which prevents the device from receiving GPS information. Another embodiment is described paragraph 18 on page 4, specifically an active jammer module that prevents the device from receiving information.

Claim 1 further defines a testing part that carries out at least one test. See paragraphs 14 and 15, page 3 lines 12-25.

Claim 4 requires operating a cellular phone in a first mode in which a position is detected and sent. This is described the last three lines of page 2. Claim 4 defines an action which prevents the position of the cellular phone from being detected, see page

2 line 4 from the bottom. Claim 4 also requires testing the privacy, see paragraphs 14-15, page 3 lines 12-25.

Claim 9 defines an electronic device with a cellular phone that has a position detection module, see page 2 line 7 from the bottom, and an position privacy control formed of a single button that prevents the position detection module from reporting information. In general, see paragraph 11 extending from page 2 up to page 3. Claim 9 further defines a testing part. See paragraphs 14 and 15, page 3 lines 12-25.

Claim 10 requires telephone electronics that enables communication and a position detection module that determines the position of the portable phone, see generally paragraph 11, page 2-3. Claim 10 further defines a testing. See paragraphs 14 and 15, page 3 lines 12-25.

Claim 20 defines an electronic device with a telephone and a position detection module, see generally paragraph 11, and a position reporting control which prevents reporting of position information, see generally paragraph 11, pages 2-3. Claim 20 further defines a testing part that tests an operation of the position reporting control. See paragraphs 14 and 15, page 3 lines 12-25.

Grounds of Rejection to be Reviewed on Appeal

Claims 10-13, 15, 17-20, 23-27 and 52 stand rejected under 35 USC 112, first paragraph, as allegedly not supporting the "testing part…" .

Claims 5-13, 15, 17-20, 23-27 and 52 stand rejected under 35 USC 112, first paragraph, as allegedly not being supported by an adequate written description.

Claims 5 and 10 stand objected to as allegedly introducing new matter.

Claims 9-13, 15, 17-19 and 51-52 stand rejected under 35 USC 112, second paragraph, as allegedly being "indefinite".

Claims 1, 2, 4-7, 9, 10, 13, 17-20, 23-27 and 51 stand rejected under 35 USC 103a as allegedly being unpatentable over Zellner in view of Simms and Mohan.

The rejection of dependent claims 11, 12, 15 and 52 based on Zellner in view of Simms and Mohan and Roeder or Altidor is incorrect for similar reasons to those discussed above.

Argument

Rejections Under Section 112

Claims 10-13, 15, 17-20, 23-27 and 52 stand rejected under 35 USC 112, first paragraph, as allegedly not supporting the "testing part…" and/or not providing an adequate written description.

This contention is respectfully traversed, since a "test module 250" is disclosed in paragraphs 14-15 of the original specification. This section discloses a test module that can be used to test a degree of privacy. The test module "is connectable to the server 260" and "runs a software layer 255 which can be updated … e.g., over the internet". The test module can connect to the server and can obtain information used for an evaluation of the degree of position blocking.

The rejection states that there is no enablement for a testing part, but the test module clearly meets this limitation. Paragraph 15 explains that this tests the operation of the security. Similarly, the "testing part" throughout these claims, quite clearly is met by paragraphs 14-15.

The rejection states that the specification does not describe the testing part "tests a privacy of said communicating electronics". In order to explain this, consider the specification as a whole. First, consider the title of the specification "position privacy in an electronic device". The summary of the invention, paragraph 5 explains that the device "enhances privacy in such a system". This device hence prevents the electronic device from transmitting its position. To quote from paragraph 5 "this hence allows selection of an enhanced privacy mode". The ways in which the enhanced

privacy mode can be selected are, as noted by the office action, a position blocking control/override, or a manual shield.

Paragraph 12 explains that hackers might or others might to determine position surreptitiously. As explained in paragraph 12 "doing this... may have serious privacy implications". The test module described in paragraphs 14 and 15 describes returning ways of hacking the position detection which can be used by the test module to evaluate the privacy. Paragraph 15 describes that request for position location can be sent to the phone, in another embodiment and the information is evaluated by the server.

The official action, however, states that the specification does not reasonably provide enablement for a testing part that tests a privacy of said communicating electronics". However, this is precisely what is described in paragraphs 14 and 15. It even states testing a degree of privacy "associated with the electronic device". It clearly states in context that this communicating electronics is the part that is being tested. To the extent that the rejection fails to teach a person having ordinary skill in the art how to make and use this system, consider paragraph 15 which explains that the server can actually request the phone to determine its position, and then evaluate whether the position has actually been returned. Certainly this is one way of testing that a person having ordinary skill in the art would certainly be able to implement.

As part of this rejection, the rejection states that claim 5 is "considered new matter" since the specification failed to provide teaching using a test that is initiated from a remote location. This again is respectfully traversed, since paragraph 15 describes the test module "sends a request for position location to the phone". Hence,

this is quite clearly initiated from a remote location.

Claim 10 stands objected to based on the contention that the specification does not include testing the communication electronics. However, this fails to reasonably read the whole claim which requires that the information is used to test the privacy of the communicating electronics. The test of that privacy has been disclosed, and this has been shown in detail above.

The antecedent basis raised in claim 9 is well taken, and will be addressed when these other issues have been completed.

The quote from claim 10 of "the testing part that provides information... used to test a privacy of said communicating electronics" has been described in detail above. The test module tests the privacy of the communicating electronics.

The antecedent issues in claims 15, 23 and 52 will be handled after the other issues noted herein have been decided.

With all due respect, therefore, it is respectfully suggested that each of these rejections are in the error and should be withdrawn.

Rejections Under 35 USC 103

Claims 1, 2, 4-7, 9, 10, 13, 17-20, 23-27 and 51 stand rejected under 35 USC 103a as allegedly being unpatentable over Zellner in view of Simms and Mohan. This contention is respectfully traversed.

In summary, no prior art suggests testing whether the position detection function has been properly blocked, or even that there would be any merit in so testing.

Zellner teaches a basic location blocking service for a wireless network. As admitted by the official action, Zellner does not disclose any about the claimed testing part.

The secondary reference to Simms has a test button that initiates a self test of the device. However, that test is described only in the following places within Simms.

"The push buttons 33 are used to manually initiate and confirm specific help requests or a self-test." (column 5, lines 41-42)

"Finally, the sixth push button is marked "TEST" and is provided to initiate a self-test of the mobile security assembly 30. "(column 6, lines 48-50)

"In step 518, the remote sensors 41 and the push button switches 33 are sequentially polled to determine whether a personal security situation exists or whether system test has been initiated. If neither, and the elapsed time counted at the internal timer has not expired, then the program repeats step 518." (column 11 line 65 – column 12 line 2)

If system test is initiated at step 518B, then the program jumps to step 534 and the self-test routine illustrated in steps 534-564 is conducted. (column 12, lines 48-50)

The test "560" is a position locator test that determines only the "position receiver working". See 564.

Therefore, the rejection reasons that the hypothetical combination of Zeller/Simms could provide a self test. However, this would be a test of whether the position locator was working properly. The present application defines just the opposite - - testing whether the position locator is BLOCKED. In fact, Simms, teaches away from testing blocking of the position locator. Simms teaches testing whether the circuits work properly. Not testing whether the functions have been BLOCKED, as claimed.

The tertiary reference to Mohan discloses position detecting operation, and a self

test loop. (column 5, lines 61 etc) testing operation and validity of operation of the communicated message that includes position information. Mohan teaches a test of communication, and also teaches E-911. The test loop determines whether "all aspects of the system are functioning properlY, including the satellite receiving capabilities, mobile telecommunications… and power management". It does not teach determining whether position reporting has been successfully blocked.

Therefore, the hypothetical combination might teach a Zellner type system with the ability to test communication information from Simms, coupled with a self test system as in the Simms reference and with a communication test as in Mohan.

However, there is no teaching or suggestion of testing whether the position detection "is actually prevented said position detection module from reporting its position", as claimed by claims like claim 1, or other similar important features defined by other claims. Therefore, the important feature of these claims is not disclosed by the hypothetical combination of prior art.

The rejection states that operation of the testing function during the privacy mode would be a "predictable result, testing of the location blocking function…". However, this conclusion is entirely based on hindsight – and this conclusion is made possible only based on the teaching of the present specification.

Communication might be tested as taught by the prior art. However, no one, prior to the present application ever realized that position privacy controls might be hackable. The normal expectation might be that once you initiate position privacy (e.g., in the language of claim 1, "prevent[ ] said position detection module from reporting its position", that the position reporting is really blocked.

The unobvious part of the claims like claim 1 and others – what if the system has been hacked or otherwise compromised – and someone could actually track you even after you thought you had prevented the reporting of position? No one has suggested that this problem could even exist, much less suggested a solution to the problem. The mere testing of whether the circuitry was operating, as done by Simms/Mohan, would not detect this kind of hack.

So, here, as in *EIBEL PROCESS CO. v. MINNESOTA & ONTARIO PAPER CO.*, 261 US 45 (1923), part of the patentable advance is the discovery of the problem itself: specifically of testing against hacking or otherwise defeating the position reporting security part (e.g., using the words of claim 1). No one has ever suggested testing this of the operation of the location blocking function. The conclusion in paragraph 17 that this would be a predictable result is actually completely unsupported by any evidence in the case. In fact, no prior art has even ever suggested this problem. Certainly no one has suggested that this could be tested in this way.

Claim 1 defines, therefore, a testing part that "carries out at least one test that forms data that indicates if said security part is actually preventing said position detection module from reporting its position". As described above, nothing in the prior art has ever even suggested that such a test would even be necessary or desirable. No prior art had ever even suggested the source of the problem that is being solved here. Accordingly, the shows clear unobviousness of the currently claimed testing using the rationale in *Eibel Process*.

Moreover, consider the so-called KSR factors, set forth in Federal Register volume 72 number 195. None of these factors would be a proper basis for rendering

obvious claim 1 (or the other claims herein.

-Rationale A is combining prior art elements according to known methods to yield predictable results. As described above, there are no known methods for combining these prior art elements: the source of the problem was not known prior to the disclosure in this application. In any case, even if the prior art is combined as suggested by the official action, nothing in this hypothetical combination of prior art suggests a test that forms a result that indicates if the security part is actually preventing the position detection module from reporting its position as claimed.

-Rationale B is substitution of one known element for another to obtain predictable results. Here, there is nothing predictable about the results, and in any case no substitution could possibly lead to these results.

-Rationale C is use of known techniques to improve similar devices in the same way. Here, the prior art shows communication devices and position reporting devices. The known techniques use self test of communications systems, and other similar systems. There is nothing that suggests the claimed specific way of improving the operation of the device: quite simply this is a new way of improving the device not suggested or disclosed by the cited prior art.

-Rationale D is applying a known technique to a known device to yield predictable results. The devices here are not known, and the result is not predictable: the source of the problem, in fact, was not known before the disclosure thereof by the applicant.

-Rationale E - obvious to try - is inapplicable since there are not here a finite number of identified predictable solutions.

-Rationale F is known work in one field being applicable to another field. Here, there is

a new problem, not suggested by the prior art, and no showing that any problem in any other field could be applied to this field.

-Rationale G is the teaching, suggestion, or motivation test. Here, there is no teaching, suggestion or motivation of this system in the prior art.

For all of these reasons, it should be seen that the present system is wholly unobvious based on the cited prior art and that claim 1 should be allowable along with the claims that depend therefrom.

The other claims should be similarly allowable.

Claim 4 defines testing the cellular phone to determine whether the position is actually being prevented from being reported. The nonobviousness of this feature has been discussed above, and claim 4 should hence be allowable for these reasons.

Claims 5-8 were not rejected over prior art.

Claim 9 defines an electronic device with communicator, and a position privacy control that "prevents position reporting by said position detection module". This is not made obvious by the prior art; in fact the prior art does not even suggest any kind of need for this kind of control.

Claim 10 defines that the testing part provides information from a remote source accessed using the communicating electronics, the information being used to test the privacy of the communicating electronics. None of the cited prior art teaches or suggests or makes obvious such a system. The dependent claims should be allowable for reasons discussed above.

Claims 17-19 were apparently not rejected based over prior art and are presumably allowable other than the section 112 issues discussed above.

Claim 20 defines a testing part that operates by communicating with a remote location, the nonobviousness of which has been disclosed in detail above. The dependent claims should be similarly allowable.

The rejection of dependent claims 11, 12, 15 and 52 based on Zellner in view of Simms and Mohan and Roeder or Altidor is incorrect for similar reasons to those discussed above.

Therefore, and for reasons stated above, the rejection does not meet the Patent Office's burden of providing a prima facie showing of unpatentability.

Please apply any charges not covered, or any credits, to Deposit Account No. 50-1387.

Respectfully submitted,

Date: __9/22/2008_____

___/Scott C Harris/_____
Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 756-7717

Attachments

Claims Appendix
Evidence Appendix (None)
Related Proceedings Appendix (None)

CLAIMS APPENDIX

1. An apparatus, comprising:

a communicating device having a position detection module therein which determines a position of said communicating device and reports information indicative of said position of said electronic device to a remote object;

a security part that is actuated to enhance privacy and which, in response to actuation of said security part produces a signal state that prevents said position detection module from reporting its position, but which allows other parts of said electronic device to operate; and

a testing part, that carries out at least one test, which forms data that indicates if said security part is actually preventing said position detection module from reporting its position.

2. An apparatus as in claim 1, wherein said position detection module is a satellite positioning system receiver.

4. A method, comprising:

operating a cellular phone in a first mode in which its position can be detected by an automatic position sensing device and automatically reported to a remote location;

responsive to an action by a user of a specific type that is made to enhance privacy, operating said cellular phone in a second, privacy enhanced mode, in which

cellular phone functions can be used to place and/or receive calls, but a position of said cellular phone can not be automatically detected by said automatic position sensing device; and

further comprising testing said cellular phone while operating in said second, privacy enhanced mode, to determine whether said position of said cellular phone is actually being prevented from being reported to said remote location .

5. A method as in claim 4, wherein said testing comprises using a network based service to test, using a test that is initiated from a remote location over the same communication channel that is used for said cellular operation, whether said position is being prevented from being reported.

6. A method as in claim 5, wherein said network based service updates software that carries out said testing.

7. A method as in claim 6, wherein said update software comprises adding information indicative of new techniques of causing said position to be reported while in said second privacy enhanced mode.

8. Canceled.

9. An apparatus, comprising:

an electronic device including a portable communicator, having a position detection module therein which determines a position of said electronic device and is capable of reporting information indicative of said position of said electronic device to a remote object;

a position privacy control that prevents position reporting by said position detection module; and

a testing part, operating to test said position privacy control carried out by said position privacy module, said testing part carrying out a test, which determines if said position privacy control has successfully prevented said position detection module from reporting its position.

10. An apparatus, comprising:

a portable communicating device, including:

(1) communicating electronics enabling communication;

(2) a position detection module therein which enables determining a position of said communicating device as a determined position; and

(3) a testing part that provides information, from a remote source that is accessed using said communicating electronics, wherein said information is used to test a privacy of said communicating electronics.

.

11. An apparatus as in claim 52, wherein said override control prevents said position detection module from determining said determined position.

12. An apparatus as in claim 52, wherein said operating said override control allows said position detection module to determine said determined position, but prevents said reporting device from reporting said information indicative of said determined position.

13. An apparatus as in claim 10, wherein said position detection module includes a satellite positioning system device.

15. An apparatus as in claim 52, wherein said information includes test software that tests proper operation of said override control.

17. An apparatus as in claim 15, wherein said information includes a result of a test that was carried out from a remote server attempting to access information from said reporting device.

18. An apparatus as in claim 15, wherein said test includes updating a program used to carry out said test.

19. An apparatus as in claim 18, wherein said update includes suggested hacks to said override control.

20. An apparatus, comprising:

an electronic device including a telephone having a first electronics module, and a position detection module therein which determines a position of said electronic device and produces a signal for reporting information indicative of said position of said electronic device to a remote object; and

a position reporting control, which prevents reporting of position information; and

a testing part, that tests an operation of said position reporting control by communicating with a remote location using said electronics module, and determining, using said communicating, if said position has been reported.

23. An apparatus as in claim 20, wherein said position reporting control prevents said position reporting device from reporting information indicative of the determined position.

24. An apparatus as in claim 20, wherein said electronics module includes communication circuitry, which continues to operate after said position reporting control prevents said reporting.

25. An apparatus as in claim 24, wherein said apparatus includes a portable telephone, and said first electronics module includes circuitry associated with said portable telephone, including circuitry for communicating with a base station associated with the telephone.

26. An apparatus as in claim 20, further comprising an indicator, which indicates a state of said position reporting control.

27. An apparatus as in claim 26, wherein said indicator is an optical indicator.

51. An apparatus as in claim 9, wherein said testing part operates over a network connection that is accessible by said portable communicator.

52 An apparatus as in claim 10, wherein said communication electronics further comprising a reporting device which reports information indicative of said determined position of said portable telephone to a remote object; and a manually operable override control, associated with said portable telephone, operating in response to a manual press of a single button on the portable telephone to request privacy enhancement to prevent said reporting device from reporting any information indicative of the determined position in any mode of operation of said portable telephone, but allowing said telephone electronics to continue to operate.

Evidence Appendix

(None)

Related Proceedings Appendix

(None)